ECHU.ORG

Règles principales pour sécuriser Windows NT, 2000 et XP.

Ce document fait le point sur les 20 principales choses rendant votre système Windows plus sécurisé, incluant aussi bien la détection que la prévention. Les points ne sont pas abordés par ordre d'importance.

Il se peut que celui-ci contienne quelques erreurs, dans ce cas n'hésitez pas à me contacter.

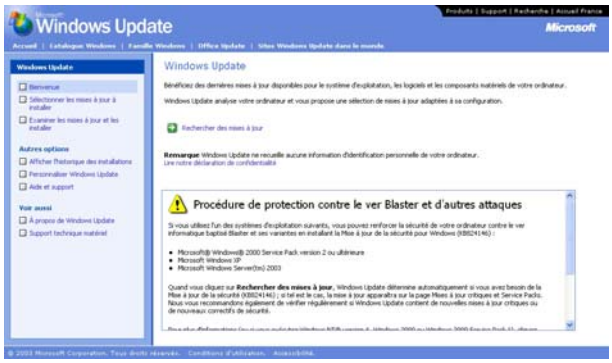
David Suzanne
das@echu.org

ECHU.ORG

Les 20 règles fondamentales

1. Installer les derniers service packs et mises à jour via Windows Update :

Aperçu de windows update :



Pour mettre à jour votre système, si vous ne savez pas comment faire, suivez les instructions contenues dans Le Guide Ultime de Windows Update :

Lien : http://www.echu.org/articles/securite/guide-windows-update.pdf

2. Utiliser NTFS à la place de FAT :

NTFS permettant de configurer les permissions et de réaliser un audit. Pour savoir si votre lecteur est configuré pour utiliser NTFS, dans l'Explorateur Windows, sélectionnez le lecteur et ouvrez ses feuilles de propriétés. Le type de système de fichiers est répertorié sous l'onglet Général.

Convertir une partition FAT32 en partition NTFS :
- menu démarrer, Exécuter...,
- taper cmd,
- appuyer sur Entrée.

Dans la fenêtre en mode texte :
- taper convert X: /FS:NTFS,
(remplacer X par la lettre de la partition que l'on veut convertir)
- appuyer sur Entrée.

3. Renommer le compte "administrateur" :

Une attaque commune consiste à utiliser un dictionnaire ou une attaque brute force sur le compte "administrateur".

Lien : http://www.echu.org/articles/attaque/techniques-vol-passwords.pdf

4. Créer un nouveau compte nommé "administrateur" :

Pour détecter les tentatives d'intrusions. Vous pouvez détecter les tentatives d'intrusions avec la version Windows de Snort (IDS gratuit).

Vous trouverez divers interfaces utilisateurs, qui vous faciliteront la prise en main, dont IDScenter.

Aperçu de IDScenter :

Lien : http://www.echu.org/articles/securite/snort-win32.pdf

5. Désactiver le compte "invité" :

Vous pouvez aussi vouloir changer le nom. Une fois que vous avez renommé le compte "invité", vous pouvez également créer un nouveau compte nommé "invité" pour détecter les tentatives d'intrusions.

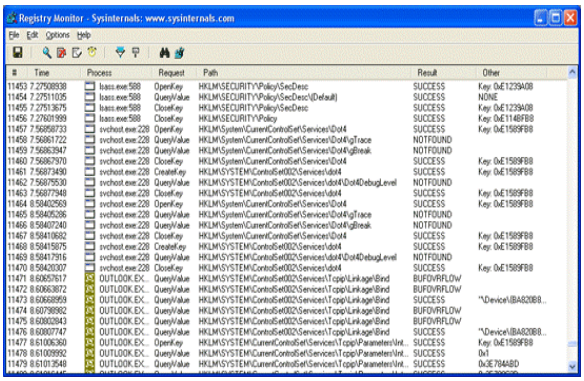
Voir régle 4 pour un utilitaire de détection d'intrusion (IDS) gratuit.

6. Lancer l'écoute de "HKEY_LOCAL_MACHINE\Security" :

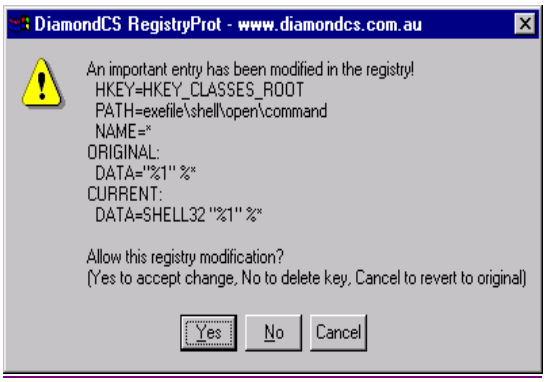
Ceci afin de détecter l'exploration du registre à distance.

Deux logiciels gratuits permettent de surveiller aisément le registre, RegistryMonitor et RegistryProt.

Aperçu de Registry Monitor :



Aperçu de RegistryProt :



Registry Monitor : http://www.sysinternals.com/ntw2k/source/regmon.shtml
RegistryProt : http://www.diamondcs.com.au/web/htm/regprot.htm

7. Activer la protection par mot de passe de l'écran de veille :

Pour ceci, dans le Panneau de configuration, ouvrez le composant Affichage. Sous l'onglet Écran de veille, en dessous d'Écran de veille, choisissez un écran de veille dans la liste puis activez la case à cocher Protégé par mot de passe.

Note : Ceci ne permet de protéger que localement.

8. Désactiver le partage automatique de ADMIN$, C$, D$, etc. :

Cette opération sera faite via le paramètre "AutoShare" dans le registre. AutoShare créé automatiquement des partages cachés sur les disques locaux. Cette valeur n'affecte pas les partages créés manuellement.

Pour un serveur :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\

En utilisant regedit, ouvrir ou créer la valeur REG_DWORD "AutoShareServer" et lui donner la valeur "0".

Pour une station de travail :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\

En utilisant regedit, ouvrir ou créer la valeur REG_DWORD "AutoShareWks" et lui donner la valeur "0".

9. Installer un logiciel firewall et un antivirus :

Cela vous permettra de surveiller et bloquer les connexions, tout en vous protégeant des différents virus qui pullulent sur la toile.

Deux produits phares, le firewall ZoneAlarm et l'antivirus Avast! sont disponibles en version gratuites pour les utilisateurs maison.

Aperçu de ZoneAlarm :

Aperçu de Avast! :

Liste de Firewalls : http://www.firewall-net.com/
Liste d'Antivirus : http://www.microsoft.com/IntlKB/France/articles/F49/5/00.ASP

10. Désactiver les connexions anonymes :

Celles-ci peuvent provoquer des problèmes de sécurité, sur vos serveurs, en particulier ceux qui sont exposés sur Internet.

Pour ce faire, rendez vous sur :

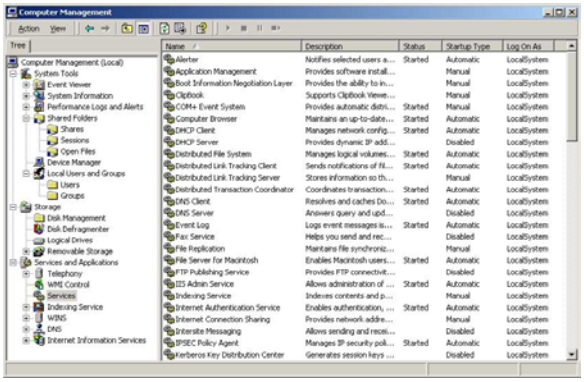
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

En utilisant regedit, ouvrir ou créer la valeur REG_DWORD "RestrictAnonymous" et lui donner la valeur "1".

11. Désactiver les services dont vous n'avez pas l'utilité :

Peu de personnes se soucient de savoir quels services tournent sur leur poste et ceci est un bien grand mal, regarder de prés chaque service est une tâche qu'il faut absolument accomplir.

Aperçu des services Windows :



Lien : http://www.hsc.fr/ressources/breves/min_srv_res_win.html

12. Déclarer chaque machine avec son adresse MAC :

Sur tout réseau avec routeur en DHCP server, ceci permettra d'éviter d'éventuelles failles de sécurité.

Lien : http://gilisa.assysm.com/win2ksrv/confdhcp/

13. Désactiver le partage de fichiers :

Ceci si vous êtes sur un poste isolé. En revanche si vous êtes en réseau, créez à la racine du disque dur un répertoire que vous partagerez, et protégez immédiatement son accès par un mot de passe. Ce répertoire devra accueillir tous les fichiers que vous voulez mettre en commun et/ou échanger avec d'autres utilisateurs.

Windows NT :
- Faire un clic droit sur l'icône du "Voisinage Réseau" situé sur le bureau.
- Cliquer sur "Propriétés"
- Depuis l'onglet "Services", cliquer sur "Interface NetBIOS"
- Cliquer sur "Supprimer" puis "OK"

Windows 2000 :
- Faire un clic droit sur l'icône des "Favoris réseau" situé sur le bureau.
- Cliquer sur "Propriétés"
- Dans la fenêtre "Propriétés de Connexion au réseau local", désélectionner l'option "Partage de fichiers et d'imprimantes pour les réseaux Microsoft"
- Sélectionner "Protocole Internet (TCP/IP)"
- Cliquer sur "Propriétés"

Windows XP :
- Aller dans les propriétés de la connexion utilisée
- Cliquer sur l'onglet "Gestion des Réseaux".
- Sélectionner "Protocole Internet (TCP/IP)" puis cliquer sur le bouton "Propriétés".
- Cliquer ensuite sur "Avancé..."
- Cliquer sur "Désactiver NetBIOS TCP/IP", puis cliquer sur "OK".

14. Ne pas stocker localement votre «hashe» :

Pour tout ceux qui emploient Lan Manager avec XP, vous savez que le « hash code » des mots de passe Lan Man ne résiste pas plus d'une heure face à un Brute Force.

Pour ce faire, vous pouvez ajouter une clé dans le registre dans :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\

En utilisant regedit, ouvrir ou créer la valeur REG_DWORD "NoLMHash" et lui donner la valeur "1".

15. Protéger le fichier win/system32/config/SAM :

Ceci est possible en empéchant le boot sur un autre periphérique que le disque où votre systeme est installé, en protégeant par mot de passe l'accés au bios, et en vérrouillant le boitier de l'unité centrale pour éviter le reset des paramètres bios (et du password).

16. Désactiver les extensions de fichiers cachées :

Tous les systèmes d'exploitation Windows cachent les extensions des fichiers dont le type est connu par défaut. Cette fonctionnalité peut être utilisée par les auteurs de virus et les pirates pour masquer leurs programmes malicieux en les faisant passer pour d'autres formats de fichiers comme du texte, de la vidéo ou des fichiers audio.

Dans une fenêtre Windows :
- Menu Outils, Options des dossiers...,
- Onglet Affichage,

Dans Paramètres avancés :
- Cocher Afficher les fichiers et dossiers cachés,
- Décocher Masquer les extensions des fichiers dont le type est connu,
- Décocher Masquer les fichiers protégés du système d'exploitation.

17. Faire des sauvegarde régulières des données critiques :

Ainsi qu'un disque de boot au cas où votre ordinateur serait abimé ou compromis.

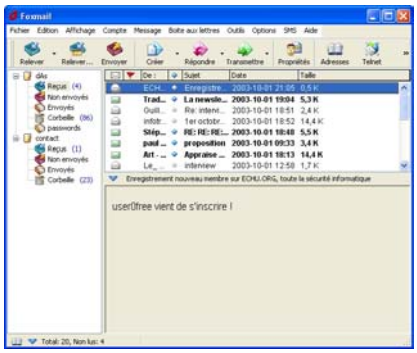
Logiciels de sauvegarde gratuits : http://www.framasoft.net/all-rubrique34.html

18. Afficher les emails uniquement en texte :

Cette opération se fait en configurant les options de votre client email afin d'éviter l'execution automatique de code et l'exploitation de failles de sécurité. Il est également conseillé d'éviter les clients emails fréquemment sujets aux failles de sécurité tels que Outlook.

Foxmail constitue une excellente alternative gratuite, de plus il utilise un filtre bayesien pour contrer le spam plus efficacement.

Aperçu de Foxmail :



Foxmail : http://foxmail.free.fr

19. Désactiver la fonction de Windows Scripting Host :

Ceci afin de prévenir l'exécution des virus écrits en Visual Basic script comme VBS_LoveLetter par exemple. Ainsi ces virus ne peuvent pas s'activer, se diffuser ou causer des dommages aux fichiers.

Pour celà, allez dans:
- Menu Démarrer,
- Paramètres,

Dans Panneau de configuration :
- Ajout Suppression de programmes
- Installation de Windows
- Accessoires
- Détails
- Décochez Exécution de scripts

Note : Un PC d'une utilisation "classique" n'a pas besoin du Windows Scripting Host (WSH).

20. Choisir des mots de passe efficaces :

La protection par mot de passe est la plus ancienne mais aussi la plus commune. Logiquement c'est également contre ce type de protection que l'on trouve le plus d'attaques. Cette règle arrive en dernier mais n'est pas la moins importante, au contraire.

Il est donc très important de choisir des mots de passe qui résisteront aux attaques brute force et autres dictionnaires. Ces mots de passe devront, de plus, être changés réguliérement.

Lien : http://www.echu.org/articles/securite/creer-password-efficace.pdf

Autres ressources

1. Sur le format NTFS :

Choix entre NTFS, FAT et FAT32 :
http://www.trucs-et-astuces-windows.com/ntfs/choix_ntfs_fat.php

NTFS sous Windows 2000 :
http://www.microsoft.com/windows2000/fr/advanced/help/ntfs.htm

2. Sur les systémes de detection d'intrusions :

FAQ : Network Intrusion Detection System :
http://www.robertgraham.com/pubs/network-intrusion-detection.html

Intrusion Detection FAQ :
http://www.sans.org/resources/idfaq/

SecurityFocus IDS :
http://www.securityfocus.com/ids

Liste de produits IDS :
http://www.securite.teamlog.fr/publication/6/12/index.html

Introduction aux systémes de detection d'intrusions :
http://www.echu.org/articles/securite/introduction-ids.pdf

3. Sur les logiciels Firewalls :

SecurityFocus Firewalls :
http://www.securityfocus.com/firewalls

[FAQ]fr.comp.securite : Les firewalls :
http://www.usenet-fr.net/fur/comp/securite/firewall.html

Mémoire technique : Ecriture d'un Firewall en Java
http://www.echu.org/articles/securite/Firewall.pdf

4. Sur les logiciels Antivirus :

[FAQ]fr.comp.securite.virus :
http://www.lacave.net/~jokeuse/usenet/faq-fcsv.html - a3

Logiciels Antivirus gratuits :
http://www.framasoft.net/rubrique54.html

5. Sur la sécurité sous Windows NT :

Windows NT - installing and securing :
http://www.securityfocus.com/infocus/1344

NT Security - Frequently Asked Questions :
http://www.it.kth.se/~rom/ntsec.html

Guide de sécurité Windows NT :
http://www.echu.org/articles/securite/NSAguide.pdf

6. Sur la sécurité sous Windows 2000 :

Hardening Windows 2000 :
http://www.systemexperts.com/win2k/hardenW2K13.pdf

Windows 2000 Security Services :
http://www.microsoft.com/windows2000/technologies/security/default.asp

Sécurisation d'un serveur Windows 2000 :
http://www.edelweb.fr/OSSIR/SecurisationWin2K.pdf

7. Sur la sécurité sous Windows XP :

Guide to securing Microsoft Windows XP :
http://nsa2.www.conxion.com/winxp/guides/wxp-1.pdf

Windows XP et la sécurité :
http://www.microsoft.com/france/WINDOWS/xp/securite/default.asp

Etat des lieux de la sécurité sous Windows XP :
http://www.ossir.org/jssi/jssi2002/supports/2B-SecWindows-Edelweb.pdf

Guide de sécurité pour WinXP Pro :
http://geeksasylum.free.fr/articles/systeme/guide_securite_windows_xp_pro/part01.htm

Informations

1. Reproduire ce document :

2. Crédits :

Auteur : David Suzanne (das@echu.org)
Source : http://www.echu.org/

Remerciements à Le_PoUnT, Magistrat, McPeter et LordCrashandDie pour leurs conseils et aides diverses.